UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/809,030	03/16/2001	Yuval Ben-Itzhak	58525.00004.UTL1	5590

36183 7590 03/08/2007

PAUL, HASTINGS, JANOFSKY & WALKER LLP
P.O. BOX 919092
SAN DIEGO, CA 92191-9092

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/809,030	BEN-ITZHAK, YUVAL	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *5-10, 13-14, 17-19, 23-24, 44-45* is/are allowed.

6)☒ Claim(s) *1-4,11,12,15,16,20-22,25-29,32,33,36,37,41-43 and 46-54* is/are rejected.

7)☒ Claim(s) *30,31,34,35 and 38-40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20070304*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-4, 11-12, 15-16, 20-22, 25-29, 32-33, 36-37, 41-43, 46-54 are rejected under 35 U.S.C. 102(e) as being anticipated by Reshef(6,584,569).

3. As per claim 1, Reshef discloses a method for protecting an application(i.e. web application) from executing an illegal or harmful operation request received from a distrusted environment, because Reshef discloses detecting security vulnerabilities(illegal or harmful) in a HTML based web application(see col. 3, lines 43-46). Reshef discloses that in the web environment the application scanner analyzes messages between a client browser and a server, these client or external clients(i.e. distrusted environment)(see col. 2, lines 16-30). Reshef discloses designating an application path of an application as restricted(see col. 3, lines 49-67, col. 4, lines 1-8), matching an operation request to the application path, wherein the application path is represented as a subdirectory of the application(see col. 8, lines 61-67, col. 9, lines 1-3, col. 3, lines 49-67, col. 7, lines 37-50), determining whether the operation request is illegal or harmful to an environment of the application according to security settings designated for the application path(see col. 3, lines 49-67, col. 4, lines 1-8, 20-32), preventing the application from executing the operation request(see col. 3, lines 1-5, col. 9, lines 60-67, col. 10, lines 1-48).

4. As per claim 2, Reshef discloses wherein the illegal and harmful operation allows unauthorized access to a computer system of the application(see col. 2, lines 56-67, col. 3, lines 1-5).

5. As per claim 3, Reshef discloses wherein said illegal and harmful operation request is application vulnerability(see col. 2, lines 56-59).

6. As per claim 4, Reshef discloses wherein said step of preventing includes the step of rejecting said illegal or harmful operation request(see col. 10, lines 26-35, 40-48).

7. As per claim 11, Reshef discloses wherein said step of determining comprises the steps of: comparing said operation request against stored known vulnerability patterns to determine a match; and blocking said operation request if said match is found(see col. 8, lines 61-67, col. 9, lines 1-31).

8. As per claim 12, Reshef discloses the step of: updating said stored vulnerability patterns with newly found vulnerability patterns(see col. 8, lines 36-46).

9. As per claim 15, Reshef discloses dividing said operation request into four zones(see col. 8, lines 1-7); comparing each of said four zones against stored known vulnerability patterns to determine a match; and blocking said operation request if said match is found(see col. 6, lines 1-12, col. 9, lines 32-53).

10. As per claim 16, Reshef discloses wherein said four zones represent a URI, query string, header, and body associated with said operation request(see col. 6, lines 1-12, col. 8, lines 1-7, col. 9, lines 32-53).

11. As per claim 20, Reshef discloses designating an application path of the application restricted; determining a destination of the operation request; and blocking the operation request if the destination is equal to designated path(see col. 8, lines 61-67, col. 9, lines 1-3, 31-53).

12. As per claim 21, Reshef discloses compiling a list of acceptable operation requests; and comparing said operation request to said list of acceptable operation requests(see col. 4, lines 15-19, col. 8, lines 36-51).

13. As per claim 22, Reshef discloses determining a parameter value contained within said operation request(see col. 3, lines 44-54); and applying a pre-defined rule to said parameter based on said parameter type, wherein said pre-defined rule defines one or more acceptable parameter values(see col. 3, lines 60-67, col. 4, lines 1-19).

14. As per claim 25, Reshef discloses storing said plurality of operation requests into a virtual directory(see col. 8, lines 13-20); building a dynamic range of entered values for each parameter in said plurality of operation requests(see col. 8, lines 61-67, col. 9, lines 1-3, col. 10, lines 1-20); computing an acceptable range of values for each parameter based on a statistical model applied to said dynamic range of entered values for each value(see col. 10, lines 1-35, 56-60); receiving a subsequent operation request; identifying parameter values in said subsequent operation request; and determining if said parameter values in said subsequent operation request are within said acceptable range of values(see col. 8, lines 61-67, col. 9, lines 1-3).

15. As per claim 26, Reshef et al. discloses adding said parameter values in subsequent operation request to dynamic range; adjusting said acceptable range of values for each parameter by applying said statistical model(see col. 9, lines 60-67, col. 10, lines 1-48).

16. As per claim 27, Reshef et al. discloses receiving one or more operation requests; formatting each operation request into a formatted message according to designated protocol, wherein the designation communication protocol is determined by the type of application being requested; indexing the one or more formatted messages(see col. 3, lines 44-58); translating the formatted messages into internal messages according to an encoding scheme, resolving a destination node for each operation request; storing a copy of the indexed one or more formatted messages(see col. 3, lines 60-67, col. 4, lines 1-8); applying one or more pipes to each operation request, wherein the number and types of pipes applied to each operation request are based on said resolved destination node of each operation request(see col. 4, lines 1-30).

17. As per claim 28, Reshef discloses wherein the designated communications protocol is http(see col. 4, line 3, 10, 16).

18. As per claim 29, Reshef discloses inherently teaches wherein said encoding scheme is ASCII, because Reshef discloses teaches http application protocol(see col. 4, line 3, 10, 16), http uses ASCII.

19. As per claim 32, it is rejected under the same basis as claim 11.

20. As per claim 33, it is rejected under the same basis as claim 12.

21. As per claim 48, Reshef discloses a system for implement an application layer security layer between a trusted application and a distrusted computer environments including means for receiving an operation request for the application (see col. 2, lines 16-30); means for embedding the operation request into a data format used by the trusted application, and means for checking a contents of the operation requests to identify if the operation request is illegal or harmful to an environment of the application(see col. 3, lines 49-67, col. 4, lines 1-8, 20-32), discloses wherein

the illegal or harmful request consists of uniform resource identifier (see col. 6, lines 1-12, 49-56).

22. As per claim 49, Reshef discloses wherein said data format is selected from HTTP(see col. 4, lines 9-12).

23. As per claim 50, Reshef discloses wherein said receiving means is a queued socket server(col. 6, lines 36-49).

24. As per claim 51, limitations have already been addressed (see claim 27).

25. As per claim 52, it is rejected under the same basis as claim 49.

26. As per claim 53, it is rejected under the same basis as claim 29.

27. As per claim 54, Reshef discloses means for providing a firewall(see col. 7, lines 4-13).

28. As per claim 36, it is rejected under the same basis as claim 15.

29. As per claim 37, it is rejected under the same basis as claim 16.

30. As per claim 41, it is rejected under the same basis as claim 20.

31. As per claim 42, it is rejected under the same basis as claim 21.

32. As per claim 43, it is rejected under the same basis as claim 22.

33. As per claim 46, it is rejected under the same basis as claim 25.

34. As per claim 47, it is rejected under the same basis as claim 26.

35. As per claims 5-10, 17-19 are allowable, because prior art nor non-patent literature disclose or teach, modifying the illegal or harmful operation into a legal or harmless operation, because the prior art discloses that when an illegal or harmful operation is detected it is analyzed and logged, does not disclose modifying the operation to a legal request.

36. As per claims 13-14, are allowable, because the prior art discloses that when an illegal or harmful operation is detected it is analyzed and logged, does not disclose modifying the operation to a legal request. Claims 34-35 are objected to, because base claims rejected. Claims are allowable because of computing a hash value for every consecutive specified number of character in the operation request, and comparing every has value to stored hash values. Prior art nor non-patent literature discloses computing hash values for a number of characters, the prior art discloses looking for parameters and checking for tampering of the application, not computing a hash value for the characters. Claims 30-31 are objected to as being rejected on base claims for inspecting one or more expressions for improper syntax and characters defined, and applying the state automate to the first operation request. Claims 38-40 are objected to as being rejected on base claims for generating a reply to the operation request, prior art nor non-patent literature teaches if legal or harmless operation of the application, generating a reply.

37. As per claims 23-24 are allowable. Claims 44-45 are allowable, because base claims rejected. Claims are allowable because of decrypting values in the cookie message header and modifying the operation request to reflect the decrypted values. Prior art fails to disclose these limitations. An example of prior art that does not disclose these is Reshef. Reshef discloses cookie values are checked to see if they have been manipulated. Non-patent literature teaches cookie poisoning, which a hacker can take on another's identity online. However, prior art fails to disclose the limitations above.

Response to Applicant

38. In the Applicant's outstanding response, it is stated by the Applicant, there is no suggestion to combine Appshield with Reshef. The Applicant's arguments were persuasive, and as such the Appshield has been withdrawn by the Examiner.

39. The Applicant states that Reshef does not disclose designating an application path. The Examiner disagrees with the Applicant. Reshef discloses the scanner examines the application-level messages that flow between a web server hosting a web-based application and a client browser operating in an intended or authorized way(see col. 3, lines 44-49). This enables the scanner to discover the structure or elements of the application's interface with external clients, particularly the path and data parameters employed in the interface(see col. 3, lines 44-59). The Applicant states that the reasons to combine BRP and Reshef are improper.

40. The Applicant states that Reshef does disclose matching an operation request to the application path, wherein the application path is a virtual directory or subdirectory of the application, according to security settings designated for the application path(see lines 22-26). The Examiner disagrees with the Applicant. Appshield teaches, recognizing the intended application security policy by analyzing each outbound hypertext markup language pages. Then it enforces compliance with the policy for each incoming hypertext transfer protocol application(HTTP).

41. The Applicant states the Reshef does not disclose determining whether the application request is illegal or harmful. The Examiner disagrees with the Applicant. Reshef discloses a method for protecting an application(i.e. web application) from executing an illegal or harmful operation request received from a distrusted environment, because Reshef discloses detecting security vulnerabilities(illegal or harmful) in a HTML based web application(see col. 3, lines 43-

46). Reshef discloses that in the web environment the application scanner analyzes messages between a client browser and a server, these client or external clients(i.e. distrusted environment)(see col. 2, lines 16-30).

42. The Applicant states that Reshef does not disclose applying one or more security pipes to each operation request, wherein the number and types of pipes applied to each operation request are based on the resolved destination node of each operation request. The Examiner disagrees with the Applicant. Reshef discloses applying one or more security pipes to each operation request, wherein the number and types of pipes applied to each operation request are based on the resolved destination node of each operation request(see col. 4, lines 1-40).

43. The Applicant states that Reshef does not disclose means for embedding the operation request into a data format used by the application. The Examiner disagrees with the Applicant. Reshef discloses the html form tag in a web server message may be associated with a numeric input field(see col. 3, lines 65-67). The client browser would only accept a numeric input value(see col. 4, line 1).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

March 3, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100